CERTIFIED INFORMATION FORENSICS INVESTIGATOR

CIFI - 2.0

IISFA - POLICY

Table of Contents

The Certified Information Forensics Investigator CIFI 2.0 POLICY

The International Information Systems Forensics Association (IISFA) is the premier information technology forensics association in the world. The IISFA is a non-profit organization whose mission is to promote the discipline of Information Forensics. The IISFA is tailored for corporations and the private sector to better understand the value, process and capabilities of Information Forensics in business operations.

About IISFA

The International Information Systems Forensics Association (IISFA) is a nonprofit organization whose mission is to promote the discipline of information forensics in the form of evangelism, education, and certification.

IISFA consists of a governing body of Board of Directors that represent various areas of expertise in information forensics and a large community of Subject Matter Experts that volunteer time and expertise to further the goals of the association.

Members of the IISFA adhere to the IISFA Code of Ethics and are candidates for the Certified International Information Systems Forensics Investigator (CIFI).

About the CIFI

The Certified Information Forensics Investigator™ (CIFI) Certification is a designation earned exclusively by the most qualified information forensic professionals in the field. Along with adherence to the highest standards of ethical conduct, the CIFI epitomizes the highest standards in knowledge requirements and expertise. The CIFI encompasses multiple domains of knowledge, practical experience, and a demonstration of expertise and understanding accomplished through a rigorous exam proctored under the most controlled of environments. Unlike many vendor certifications, the CIFI maintains vendor neutrality and is independent of dependency requirements such as sponsored training, purchasing of product, or requirements other than ability. In fact, candidates may choose to sit for the exam without any restrictions other than adherence to the IISFA code of ethics and the exam fee. The CIFI is recognized as the only certification that truly represents the abilities of field information forensics investigators and is the benchmark by which they are measured. Earning the CIFI designation is a significant accomplishment and identifies the best in the profession of information forensics investigator.

The Certified Information Forensics Investigator™ (CIFI) Certification is specifically developed for experienced information forensics investigators who have practical experience in performing investigation for law enforcement or as part of a corporate investigations team. The CIFI certification is designed to demonstrate expertise in all aspects of the information investigative process and is dedicated to bringing a level of consistency to the profession than can be recognized outside the field.

IISFA certifications are globally accepted and recognized. They combine the achievement of passing an exam with credit for your work and educational experience, giving you the credibility you need to move ahead in your career. Certification proves to employers that you have what it takes to add value to their enterprise. In fact, many organizations and governmental agencies around the world require or recognize IISFA's certifications.

Independent studies consistently rate IISFA's designations among the highest paying IT and impactful certifications that an IT professional can earn. Earning and maintaining an IISFA certification:

Boosts your earning potential

Counts in the hiring process

Enhances your professional credibility and recognition

STEP 1 - IISFA MEMBER

The online registration process will enable you to register for will be a IISFA member and take the IISFA ID number.

Step 2 - Register for the EXAM

The online registration process will enable you to register for an exam, and purchase the exam voucher

Prepare for the Exam

The Candidate's Guide to the CIFI Exam provides a detailed outline of the subject areas covered on the examination, a suggested list of reference materials to review, a glossary of acronyms commonly used on the examination, and a sample copy of the answer sheet used for the exam.

The Candidate's Guide to the CIFI Exam is available through the IISFA website

CIFI Certification Job Practice

The CIFI exam covers six information forensics areas, each of which is further defined and detailed through Tasks & Knowledge statements.

These areas and statements were developed by the CIFI Certification Board and represent a job practice analysis of the work performed by information forensics investigator as validated by prominent industry leaders, subject matter experts and industry practitioners.

The following is a brief description of these areas, their definitions and approximate percentage of test questions allocated to each area.

This information provides the basis for the CIFI exam and the qualifying experience for certification.

STEP 3 - Take the exam

Candidates will be admitted to the test center only if they have a valid admission voucher and an acceptable form of identification (ID). An acceptable form of ID must be a current and original government issued ID that contains the candidate’s name, as it appears on the admission ticket, and

the candidate's photograph. The information on the ID cannot be handwritten. All of these characteristics must be demonstrated by a single piece of ID provided. Examples include, but are not limited to, a passport, driver's license, military ID, state ID, green card and national ID. Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit his/her registration fee.

Misconduct

Candidates who are discovered engaging in any kind of misconduct, such as giving or receiving help; using notes, papers, note pads or other aids; attempting to take the exam for someone else; using any type of communication device including cell phones during the exam administration; or removing the exam booklet, answer sheet or notes from the testing room will be disqualified and may face legal action. Candidates who leave the testing area without authorization or accompaniment by a test proctor will not be allowed to return to the testing room and will be subject to disqualification.The testing agency will report such irregularities to IISFA CIFI Certification Committee.

Reporting of Your Test Results

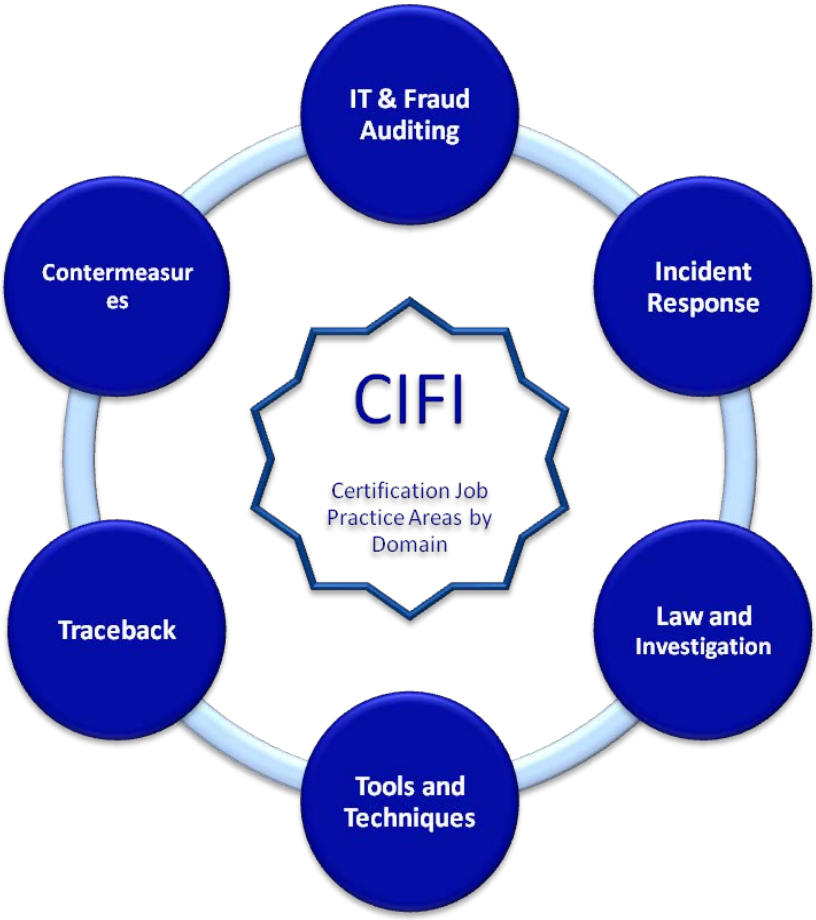
Candidate scores are reported as a scaled scored. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. IISFA uses and reports scores on a common scale from 0 to 600. For example, the scaled score of 800 represents a perfect score with all questions answered correctly; a scaled score of 200 is the lowest score possible and signifies that only a small number of questions were answered correctly. A candidate must receive a score of 420 or higher to pass the exam. A score of 420 represents a minimum consistent standard of knowledge as established by IISFA's CIFI Certification Committee. A candidate receiving a passing score may then apply for certification if all other requirements are met.

***Passing the exam does not grant the CIFI designation. To become a CIFI, each candidate must complete all requirements*.**

Retaking the CIFI Exam

A candidate receiving a score of less than 420 has not passed and can retake the exam by registering and paying the appropriate exam fee for any future exam administration. To assist with future study, the results letter each candidate receives will include a score analysis by content area. There are no limits to the number of times a candidate can take the exam.

The job practice domains and task and knowledge statements are as follows:



The CIFI exam includes six areas in its common bodies of Knoledge (CBKs), all strongly related to information forensics:

1. **IT & Fraud Auditing**
2. **Incident Response**
3. **Law and investigation**
4. **Tools and techniques**
5. **Traceback**
6. **Contermeasures**

1. IT & Fraud Auditing

The methodologies utilized to leverage audit trails/log files in various systems to determine the methods and sources of malicious activity. Included will be best practices for the configuration of the logging devices and collection of data that are admissible as evidence in legal proceedings.

- **Principles of Fraud Auditing**
  - Fraud Auditing as a detection tool
  - Fraud Auditing as an investigative tool
  - Comprehension of auditing through the OSI Model
  - Comprehension of auditing systems maintenance
- **Evaluation of audit systems architecture and product selection**
- **Types of Fraud Audit**
  - 3rd party
  - Duty rotations
  - Internal audits
- **Planning for Investigations**
  - Information Systems Secure Design
  - Physical Environment Secure Layout
  - Archiving of logging information
- **Fraud Auditing Process for Detection**
  - Review of activity
  - Anomalous patterns
  - Intrusion Detection Systems
  - Forced duty rotation
- **Auditing Process for Investigation**
  - Targeting of 'interesting' information
  - Log collection
- **Log Files**
  - Logging devices
  - Infrastructure devices
  - Security devices
  - Applications
  - Syslog servers
  - Access control systems
  - Format of Log Files
  - Information contained in log files
  - Time Synchronization
  - Multi-source data correlation
- **Fraud Auditing**
  - Principles and typical schema of financial fraud
  - Identity theft and detection mechanism
  - Technical fraud
  - Internal fraud
  - Investigation mechanism
  - Correlation procedures and tools

2. Incident Response Team

Best practice and processes for creating, organizing, development, and deploying an Incident Response Team for malicious activity.

- **Event vs. Incident**
  - Definition of Events and Incidents
  - Malicious vs. Unintentional
  - Impact to an entity

- Impact to process execution
- **Goals of malicious activity**
  - Financial gain
  - Political motivation
  - Alteration
  - Destruction
  - Access Denial
- **Profiles of malicious attackers**
  - Insider vs. Outside
  - Information Warrior
  - Cyber terrorist
  - Recreational Hacker
  - Industrial Espionage
  - Institutional Hacker
  - Aggressive Foreign Nation
- **Roles of IRT in the enterprise**
  - Disaster Recovery
  - Business Continuity
  - Malicious Activity Response
  - HR proceedings
- **Organizing an Incident Response Team**
  - Charter of the IRT
  - Skill set requirements
  - Roles and function
- **Empowerment and authority of the IRT**
  - Agent authority
  - Powers of confiscation
  - Securing corporate property
- **IRT Leader**
  - Skill requirements
  - Training
  - Authority
- **Process development and testing**
  - Process development
  - Organizational review
  - Policy review
  - Process Testing
  - Scenario Development
  - Walk Through
  - Live Fire
- **First Response**
  - Triage
  - Recovery vs. Investigation
  - Execution of correct process
- **Securing a crime scene**
  - Sequestering victims, witnesses, and suspects
  - Securing evidence
  - Arrest
  - Determination of law enforcement involvement
- **Evidence handling**
  - Labeling and logging
  - Chain of Custody
  - Storage
  - When is evidence returned to the owner
  - Preparation for analysis
  - Preparation for court
  - Child porn
  - National security
  - Authority to contact law enforcement
- **Reactive vs. Proactive investiga- tions**
- **Sting operations**

3. ***Law and Investigation***

Law , private and law enforcement investigator differences, investigation methods; evidence handling;cybercrime; probationary means ; acquisition technics;

Each chapter develops different modules focused on regional and communitarian laws .

Main principles will be introduced in this CBK are:

- **Principles of penal code procedure;**
- **Principles of civil code procedure;**
- **Ethics in information forensics activities;**
- **Law enforcement procedures, constraints, roles and responsibilities;**
- **Evidence collection requirements to produce documentation during a trial.**

4. Tools and technique

The tools and techniques employed when performing an investigation of information systems in a manner best calculated to maximize evidence recovery and permit evidence to be used in a legal venue for prosecution.

- **Recovery vs. Investigation**
- **The information forensics investigator toolkit**
  - Imaging tools
  - Hashing tools
  - Deep data recovery tools
  - Search tools
  - File systems navigator
  - File chain navigator
  - Heuristic tools
  - Communication tools
- **Setting up the information forensics lab**
  - Location
  - Security
  - Reporting capabilities
  - Evidence locker
  - Access control
  - 'Clean Rooms'
- **Evidence**
  - Electronic evidences vs. physical evidence
    - Why is electronic evidence held in significant scrutiny
    - Issues with electronic evidence handling
  - Evidence tagging and tracking
    - Material tags
    - Marking directly on evidence
    - Marking electronic evidence
    - Chain of custody
    - Details in evidence transport
    - Laws addressing electronic evidence
- **Introduction to techniques used in investigations**
  - Computer forensics vs. information forensics
    - Differences and overlap
  - Computer forensics
    - Imaging and analysis
    - Operating system dependencies in imaging
    - Disk level search and analysis
  - Information forensics
    - Remote imaging and analysis
    - Infrastructure analysis for tracing
    - Collection of remote evidence
- **Introduction to tools used in investigations**
  - Imaging tools
    - File system level imaging
    - Disk imaging
    - Bit imaging
    - Migration of images between operating platforms
  - Data recovery tools
    - Simple operating system recovery methods
    - Undelete tools
    - Rebuilding deleted files from file disk tables
    - Rebuilding files by file chains
    - Slack space recovery
  - Hashing tools
    - Evidence tagging for proper chain of custody
    - Methods of hashing and digital signature
  - File system navigation
    - File system search tools
    - Binary search tools
    - Target evidence search
  - File chain tools
    - Use in recovery
    - Issues and concern in utilization
    - Evidentiary integrity of recreated chains
  - Heuristic Tools
    - Images and stenography applications
    - Predicative analysis
- **Archiving evidence**
  - Methods of archiving
  - Maintaining chain of custody over long periods of storage
  - Length of archive time

5. Traceback

The methodologies utilized to trace a malicious attack back to its source, determine the identity of the offender through various net-based investigation techniques.

- **Principles of Traceback**
  - Reporting of Incidents
  - Traceback report vs. Investigation report
  - Level of detail
  - Confidentiality
  - Typical formats
- **Understanding The Internet**
  - Protocol
  - Basic Routing
  - Topology
  - Protocol Misuse
  - Anonymous transmissions
    - Spoofing
    - Forgery
- **Anomalous Traffic Attacks**
  - Protocol Analysis
  - Header analysis
  - Payload analysis
- **Protocols**
  - The TCP/IP Suite
  - Breaking out the packet
  - Header information
  - Payload
  - Port Services
- **Sourcing Attacks**
  - Jurisdictional issues
  - Owned network vs. Remote networks
  - Real Time Traceback
    -Active port service connections
    -Upstream connection trace
  - Back splatter from spoofed attacks
  - Cold Traceback
  - Header traceback
  - Log file analysis
- **Collaboration**
  - ISPs
  - Wiretapping laws
  - Patriot Act
  - Willingness to cooperate
  - Best approach for non-compelling information gathering
  - Private Networks
  - Rights of Privacy
- **Law Enforcement**
  - Ownership of the investigation
  - Subpoena vs. Search Warrant
- **Investigative Tools for Tracing**
  - Foot printing
  - IP Trace utilizing pubic sources of information
  - InterNIC
  - Promiscuous display of information
  - Public Domain vs. Intrusion in gathering information
  - Social Engineering
  - Legality and Ethics
  - Online investigation
  - Contacting source organization of attack
- **Reporting**
  - Investigative log
  - Details of investigation
  - Reporting Abuse to source network custodians
  - Reporting to authorities

6. *Countermeasures*

The methods and technologies involved in preparing a multi-layered defense against unwanted intrusions of information assets. The technologies involved in preparing perimeter security, transmission security, data integrity, honey pots, etc

- **Secure design and information forensics**
  - Perimeter security
  - Transmission security
  - Data Integrity
  - Holistic approach as a preventative
- **Utilizing secure design in preparation for incidents requiring investigation**
  - Enabling full auditing/logging on all systems
  - External logging systems
  - Syslog servers
  - Forensic data gathering tools
  - Time synchronization
  - Online/Nearline/Offline storage of logs
  - Usage monitoring systems
- **Lockdowns during an investigation**
  - Understanding of system lock down procedures
  - Lockdown vs. shutdown
  - Crime scene handling
    - Activation of the IRT
    - Initial triage
  - Honeypot usage for dynamic investigation
    - Methods for session handoff
    - Full session recording and monitoring
    - Dynamic traceback
- **Business continuity planning and design**
  - Utilizing during investigation and recovery process
  - Providing for evidence seizure and concurrent

STEP 4 -Maintain the Certification

The CIFI policy requires the attainment of CPE hours over an annual and three-year certification period. CIFIs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 30 CPE hours. These hours must be appropriate to the currency or advancement of the CIFI's knowledge or ability to perform CIFI-related tasks. The use of these hours towards meeting the CPE requirements for multiple IISFA certifications is permissible when the professional activity is applicable to satisfying the job-related knowledge of each certification.
- Submit annual CPE maintenance fees to IISFA international headquarters in full.(10 euro Ordinary Member – 30 euro Law enforcement member and Company member)
- Attain and report a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period.
- Respond and submit required documentation of CPE activities if selected for the annual audit.
- Comply with IISFA's Code of Professional Ethics.
- Recertification after the CIFI expired time that is 5 years
- Any certification CIFI made before 31/12/2009 will expire on 21/12/2011

Failure to comply with these certification requirements will result in the revocation of an individual's CIFI designation.

Annual and Three-Year Certification Period

The annual reporting period begins on 1 January of each year. The three-year certification period varies and is indicated on each annual invoice and on the letter confirming annual compliance.

For newly certified CIFIs, the annual and three-year certification period begins on 1 January of the year succeeding certification.

Reporting CPE hours attained during the year of certification is not required. However, hours attained between the date of certification and 31 December of that year can be used and reported as hours earned in the initial reporting period.

Payment of CIFI Maintenance Fee and Reporting of CPE Hours

Payment of the maintenance fee and reporting of CPE hours is required annually during the renewal period. Invoice notification is sent both via e-mail. Payment and reporting of CPE hours is due by 15 January to retain certification.

Payment of the annual maintenance fee and reporting of CPE can be done online at www.IISFA.org or by submitting the information on the annual renewal invoice.

Notification of Annual Compliance

CIFIs who report the required number of CPE hours and submit maintenance fees, in full, in a timely manner will receive a confirmation from IISFA. This confirmation will include the number of CPE hours accepted for the annual reporting period, hours reported for past years within the three-year certification period and the number of hours required to qualify for the fixed three-year certification period. It is the responsibility of each CIFI to notify IISFA promptly of any errors or omissions in this confirmation.

Use of CIFI Logo

Individual use of the CIFI logo (on items such as business cards, web sites, marketing or promotional materials) is not permitted because it can imply endorsement or affiliation on IISFA's behalf of that person's products or services. Individuals can use the CIFI acronym after their name (e.g., Giuseppe M.azzaraco, CIFI in lieu of the logo).

Audits Of CPE Hours

A random sample of CIFIs is selected each year for audit. Those CIFIs chosen must provide written evidence of previously reported activities that meet the criteria described in the Qualifying Professional Education Activities. Please send copies of supporting documentation since documents will not be returned. The CIFI Certification Committee will determine the acceptance of hours for specific professional educational activities. Those individuals who do not comply with the audit will have their CIFI certification revoked.

Recordkeeping

A CIFI must obtain and maintain documentation supporting reported CPE activities. Documentation should be retained for twelve months following the end of each three-year reporting cycle. Documentation should be in the form of a letter, certificate of completion, attendance roster, Verification of Attendance form (located in this policy) or other independent attestation of completion. At a minimum, each record should include the name of the attendee, name of the sponsoring organization, activity title, activity description, activity date, and the number of CPE hours awarded or claimed.

Revocation

CIFIs who fail to comply with the CIFI CPE Policy will have their CIFI credential revoked and will no longer be allowed to present themselves as a CIFI. Individuals who have their CIFI certification revoked will be required to take and pass the CIFI exam and submit a completed application for CIFI certification.

Reconsideration And Appeal

CIFIs who have had their certification revoked due to non-compliance with certification requirements may appeal such revocation by submitting a written request to IISFA. This request must be received no later than sixty (60) days after notice of revocation and include a detailed explanation for the appeal.

Qualifying Professional Education Activities

Activities that qualify for CPE include technical and managerial training. This training must be directly applicable to the assessment of information systems or the improvement of audit, control, security or managerial skills (www.IISFA.org) to ensure a proper balance of professional development is attained. CPE hours related to management skills must be relevant to management of information forensics. CPE hours are not accepted for on-the-job activities unless they fall into a

specific qualifying professional education activity. Training in basic office productivity software, such as Microsoft Word or Excel, does not qualify as CPE. Specific activities have annual CPE hour limits. The following categories of qualifying activities and limits have been approved by the CIFI Certification Committee and are acceptable for CPE.

Personal Professional Development

- **IISFA professional education activities and meetings (no limit):** These activities include IISFA conferences, seminars, workshops, chapter programs and meetings and related activities. CIFIs earn CPE hours according to the number of hours of active participation. (See Calculating CPE Hours section). Participation in IISFA chapter meetings will earn a minimum of one credit hour regardless of actual duration. Please note that chapter programs and meetings are not automatically reported to the IISFA database. Please retain proof of attendance.
- **Non-IISFA professional education activities and meetings (no limit):** These activities include in-house corporate training, university courses, conferences, seminars, workshops, and professional meetings and related activities not sponsored by IISFA. In addition, CPE hours can be earned from certification review courses if such courses advance the CIFI's IS audit, control and security or audit-related managerial knowledge or skills. CIFIs earn CPE hours according to the number of hours of active participation. (See Calculating CPE Hours section). However, successfully completed university courses in related fields, including university online courses, earn 15 CPE hours per semester credit hour and 10 CPE hours per quarter credit hour (semester = 15 weeks of class; quarter = 10 weeks of class).
- **Self-study courses (no limit):** These activities include structured courses designed for self-study that offer CPE hours. These courses will only be accepted if the course provider issues a certificate of completion and the certificate contains the number of CPE hours earned for the course.
- **Vendor sales/marketing presentations (10-hour annual limitation):** These activities include vendor product or system specific sales presentations related to the assessment of information systems.

Contributions to the Profession

- **Teaching/lecturing/presenting (no limit):** These activities include the development and delivery of professional educational presentations and the development of self-study/distance education courses related to the assessment of information systems. For presentations and courses (all types), CPE hours are earned at five times the presentation time or time estimated to take the course for the first delivery (e.g.: two hour presentation earns ten CPE hours) and at the actual presentation time for the second delivery. CPE hours cannot be earned for subsequent presentations of the same material unless the content is substantially modified. For self-study/distance education courses, one CPE hour is earned for each hour spent upgrading/maintaining the course limited to twice the estimated time to take the course.
- **Publication of articles, monographs and books (no limit):** These activities include the publication and/or review of material directly related to the information systems audit and control profession. Submissions must appear in a formal publication or website and a copy of the article or the website address must be available, if requested. For books and monographs, the table of contents and title page must be available. CPE hours are earned for the actual number of hours taken to complete or review the material.
- **Exam question development and review (no limit):** This activity pertains to the development or review of items for the CIFI exam or review materials. Two CPE hours are earned for each question accepted by an IISFA CIFI item review committee. Such hours can be multi-counted for all IISFA certifications. Actual hours will be given for the formal item review process.
- **Passing related professional examinations (no limit):** This activity pertains to the pursuit of other related professional examinations.One CPE hour is earned for each examination hour when a passing score is achieved.

- **Working on IISFA Boards/Committees (10-hour annual limitation per IISFA certification):** These activities include active participation on an IISFA Board, committee, sub-committee, task force or active participation as an officer of an IISFA chapter. One CPE hour is earned for each hour of active participation. Active participation includes, but is not limited to, the development, implementation, and/or maintenance of a chapter website. Such activities can be counted more than once toward each IISFA designation that is held.
- **Contributions to the information Forensics and control profession (10-hour annual limitation in total for all related activities for CIFI reported hours):** These activities include work performed for IISFA and other bodies that contribute to the IS audit and control profession (i.e. research development, certification review manual development, K-Net development, performing peer reviews).
- **Mentoring (10-hour annual limitation):** Certifieds are able to receive up to 10 CPEs annually for mentoring. Activities include mentoring efforts directly related to coaching, reviewing or assisting with CIFI exam preparation or providing career guidance through the credentialing process either at the organizational, chapter or individual level. The mentoring activity must be an activity supporting a specific person in preparation for their IISFA exam or certification career decisions. One CPE hour is earned for each hour of assistance.

Calculating CPE Hours

One CPE hour is earned for each fifty (50) minutes of active participation (excluding lunches and breaks) in a professional educational activity. CPE hours are only earned in full-hour increments and rounding must be down. For example, a CIFI who attends an eighthour

presentation (480 minutes) with 90 minutes of breaks will earn seven (7) continuing professional education hours.

Sample Calculation
Educational Activity Schedule Actual Hours Minutes
9:00 a.m. – 5:00 p.m. 8.0 480
Less: Two 15-minutes breaks <.5> <30>
Less: Lunch — 1 hour <1.0> <60>

Total hours of professional education activity 6.5 390

Calculation of CE Hours
390 minutes divided by 50 minutes = 7.8 or 7 CPE hours (rounded down)

Contact Information
www.IISFA.org *www.iisfa.it*

IISFA Code of Professional Ethics

IISFA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and IISFA certification holders shall:

The IISFA members contract to agree and obey to the following rules of the Code of Ethics:

1) Support and promote a right information of the practices, concepts, standards and best practice universally recognised in the field of Information Forensics.

2) Do its activities according to the best practice and the total respect of the associative rules and Policy in force in the country in which you work.

3) Maintain a right knowledge and competence level in the development of the Information Forensics practice.

4) Do its work with professionalism, responsibility, ethic and honesty.

5) Maintain the privacy about all the confidential or private information discovered during the development of the professional activities and, if necessary, of the associative activity;

6) Not to damage in any way the reputation or the professional practice of the colleagues, customers, employers and the Association;

7) Not to do activities which can be a real conflict of interests or can damage the reputation or can cause moral and material damages to the colleagues, customers, employers and the Association.

8) Not to use the name and the logos of the Association without a previous authorisation of the pro-tempore President. The name of the Association, the logo, the own associative qualification, cannot be use, advertised, shown off, promote, promised and exploited during a marketing/commercial activity or during a promotion/professional relationship without the pro-tempore President authorization, heard the opinion of the Managing Board.

9) The IISFA logo cannot be used or affixed on materials employed by the teachers and by the students to form private or public subjects without the President authorisation. The logo cannot be associated, directly or indirectly, and without the President authorisation, to other logos or symbols of societies and associations with profit and benefit aim.

10) During the development of the private or business activities, in case of request of information about the association from the interlocutor, it would be necessary to postponed to an other site or to the web site www.iisfa.it

11) Furthermore, it is not possible to use for extra-associative reasons (especially in commercial activities and direct and indirect business), the emails with @iisfa.it @iisfa.net, @iisfa.eu dominion given to partners and members of the Managing Board

12) During the development of the working activity it is not possible to use “information, studies, analysis, material and IISFA logos “, received for associative reasons, with the commercial and business intent unless with the authorisation given by the Present.

13) The members of the Managing Board, the partners with special works and functions, all the people who in any way and shape represent the Association have, the moral and legal duty, to abstain to promote, do, conclude (even on behalf of a third party) commercial activities, business or profit with anyone whom the Association is in relation, according to the no profit initiatives or following to sponsored or organised events, in order to avoid that happens conflicts of interest and that someone uses without permission privileged information learnt during the development of one’s own associative duty. All the relation of business mentioned before are not included in these hypothesis.

14) Offers of lectureship or charges received on the occasion of organised events and initiatives sponsored by IISFA, must be examined pre-emptively and authorised by the Managing Board.

15) The Association suggests, prefers and encourages the deepening of the discipline in English, in order to create a complete and functional deepening of the Information Forensics and all its aspect in international field.

16) All the behaviours opposite and contrasting with the applications, purposes and aims sponsored by the Association are forbidden by means of National and International organs.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

The Certified Information Forensics Investigator

Verification Of Atten dance For m

CIFI Continuing Professional Education

CIFI Certification Number:_____

_____ attended the following professional educational activity.

(Name)

Title:_____
_____

(Title or name of program/course)

Date(s):_____ CPE Hours Earned:_____

Sponsor:_
_____
_____

Description:_____
_____

_____
_____

_____
_____

_____
_____

Location:_____
_____

***Name of Presenter:**_____

_____

Signature:_

_____

_____

(Presenter or Authorized Person)

***Note: If you are the presenter of the professional activity, please have the course sponsor sign.**

NAME:

CIFI Certification Number:

Certification Period: to

CPE

Activity Title Sponsor Activity Description Date Hours

Support

Documents
Included
(Y/N)
NOTE: This form is meant to serve as a tool to track your annual CPE hours.
All supporting documentation must be maintained for twelve months following the end of each three-year reporting cycle.
E-mail: *certification@IISFA.it*
Web site: *www.IISFA.org www.iisfa.it*